



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,487	08/16/2001	Edward W. Kohler JR.	12221-006001	3664

26161 7590 01/14/2009
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER

ISMAIL, SHAWKI SAIF

ART UNIT	PAPER NUMBER
----------	--------------

2455

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

01/14/2009

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

RECORD OF ORAL HEARING

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex Parte EDWARD W. KOHLER, Jr., and MASSIMILIANO A. POLETTTO

Appeal 2008-3007
Application 09/931,487
Technology Center 2400

Oral Hearing Held: November 5, 2008

Before HOWARD BLANKENSHIP, JAY P. LUCAS, and
THU A. DANG, *Administrative Patent Judges*

APPEARANCES:

ON BEHALF OF THE APPELLANT:

Dennis Maloney, Esquire
FISH & RICHARDSON, P.C.
P.O. BOX 1022
Minneapolis, MN 55440-1022

1 The above-entitled matter came on for hearing on Wednesday,
2 November 5, 2008, commencing at 9:00 a.m., at The U.S. Patent and
3 Trademark Office, 600 Dulany Street, Alexandria, Virginia, before
4 Dominico Quattrociocchi, Notary Public.

5 JUDGE BLANKENSHIP: -- hearing and you have 20 minutes and
6 you begin when you like.

7 MR. MALONEY: Okay. Thank you, very much. This morning I'd
8 like to discuss Claims 1, 2, 4, 6, 9, 11, and 15. All the claims in the
9 application were -- except for Claims 13 and 14 were rejected as anticipated
10 by the Yavatkar and the, and the Claims 13 and 14 which were rejected as
11 being obvious over Yavatkar and Julie Hill (phonetic sp.) I probably will not
12 get to because the Examiner basically uses Hill for a means for classifying
13 attack severity.

14 Generally, my client's invention is directed to distribute statistical-
15 based techniques for protecting a data center against a denial of service
16 attack. Examiner relies on the Yavatkar's disclosure of watchdog and
17 bloodhound agents. According to the, the reference, a watchdog agent
18 mantra is network traffic and detects an attack and, as a result of that,
19 launches one or more bloodhound agents.

20 These bloodhound agents traverse nodes in a network to trace the
21 source of the attack, so they jump from node to node. They can either jump
22 to a node or substantiate another bloodhound agent to go to a different node.
23 So this technique requires that the watchdog agent or some other agent
24 determine that there's an attack, and also it requires that that agent determine

1 what type of attack it is in order to launch a particular type of -- so it's
2 probably only useful if the attack type is known, what type of attack.

3 In contrast, my client's invention uses data collectors to collect
4 statistical information in packets that are traveling in the network -- and
5 these data collectors are deployed at different points of the network,
6 typically at network peering points as disclosed in the specification --
7 process that information to determine if there's an attack and, based on the
8 processing of the statistical information, we attempt to find the source of the
9 attack.

10 Specifically with respect to the claims, Claim 1 includes a novel
11 feature of the action of sending queries to data collectors that are employed
12 at different points in the network, and the data collectors collect the --
13 information on the network packets sent over the network, and the queries
14 request this statistical information.

15 And then we also have the feature processing this, this statistical
16 information to determine the source of suspicious network traffic sent to the
17 data center. The Examiner tries to argue that the claim language merely
18 recites sending queries to data collectors to request statistical information
19 and does not specify the type of query. We disagree. We believe that we do
20 specify to take a query because we specify a query for statistical
21 information. Any other requirement or limitation on quote/unquote type of
22 query would only serve to narrow the scope of the claim, and, in view of the
23 Primary Reference, I don't think it's required.

24 But in any event, we consider that the Yavatkar does not describe this,
25 this technique of sending queries to data collectors for statistical

1 information. We believe that Yavatkar, if correctly read, does not describe
2 querying of anything or for anything. So that they don't describe the query
3 nor the querying for statistical information.

4 The -- rather, Yavatkar teaches that this watchdog watches these
5 specific types of bloodhounds. Based on the type of attack, bloodhounds try
6 to trace the attack by traversing from node to node. Our view is not
7 equivalent nor suggests launching -- I'm sorry -- sending the queries to data
8 collectors to try to gather information then process that information based
9 upon using any one of a number of techniques disclosed in the application to
10 determine whether or not the data center is under attack and where the attack
11 is coming from.

12 JUDGE DANG: Okay, if I may interrupt and ask for a little
13 clarification, it seems the Examiner is trying to -- I, I, guess his finding is
14 that the watchdog directs or commands the bloodhound to do these searches,
15 and then the, the bloodhound then responds by providing reports. So he's
16 saying what's the difference between these commands that, that are given to
17 the bloodhound in order to receive the response? What's the difference
18 between that and query -- and a query?

19 MR. MALONEY: Well, many differences. First of all, there really is
20 no query of the bloodhound agent. I think we can all agree on that. So the
21 Examiner is basically taking the, the action of launching or substantiating a,
22 a bloodhound agent as being the equivalent of a query; however, the claim
23 specifically talks about sending queries.

24 In a sense, sending a query, we don't receive just one report which is
25 what Yavatkar -- Yavatkar essentially sends a bloodhound agent to a node.

1 The node does some processing on that. The bloodhound agent does some
2 processing on that node, looking at the ports and the lengths that traffic is
3 being -- that they're being used in that node, and sends a report back to the
4 watchdog to say these are the ports that had certain types of traffic on it.

5 JUDGE DANG: Yeah, but --

6 MR. MALONEY: Any --

7 JUDGE DANG: But if he sends something back as a response, isn't
8 that a response to a query? I mean, wouldn't, wouldn't this command that
9 requires a response to a query?

10 MR. MALONEY: No, where is the query?

11 JUDGE DANG: Well, that's what I'm asking. If a command -- a
12 direction is sent, doesn't that require a response? Isn't that a query?

13 MR. MALONEY: No. The query, the query come -- in our system --

14 JUDGE DANG: Okay, yeah, where is the query defined? Do you, do
15 you define the query -- what is a query in your specification that say it is
16 specific? It cannot be a direction that gets a, a response.

17 MR. MALONEY: Yes, of course we do.

18 JUDGE DANG: Okay.

19 MR. MALONEY: In, in -- we -- in the claim, we say sending queries
20 to data collectors. Okay. So we don't, we don't specifically say we send
21 data query to one data collector. We send queries to data collectors, and
22 essentially what happens -- if you could imagine, in that network we have
23 data collectors which are just deployed at different points in that network
24 and the -- if we go back to say a description in the specification we have a

1 control center or possibly even a gateway sending these queries to different
2 data collectors to try to pinpoint where the attacking traffic is coming from.

3 And they may be sending -- they'll, they'll likely be sending multiple
4 queries over multiple periods of time to try to figure out where the traffic is
5 coming from. And what they're querying for are not paths that are being
6 taken by these bloodhound agents, but statistical information that's being
7 gathered on the network traffic that's going through those data collectors,
8 and none of that is described in, in Yavatkar. Yavatkar -- all Yavatkar
9 simply does is to try to figure out where -- what links and ports are
10 particularly known, and the network is talking to then try to follow those
11 paths if you will to the next node.

12 And when they find the node, it then sends a report back to the
13 watchdog saying where, where they found the node typically they
14 understand the Yavatkar is a little unclear to me, but it seems as though once
15 the watchdog agent -- I'm sorry, the bloodhound agent sends its report to the
16 watchdog agent, it then destroys itself. And the watchdog agent may send
17 out another, another bloodhound agent, or actually the bloodhound agent can
18 also substantiate itself to another node, but there's no transfer back to the
19 watchdog of statistical information. It's all path information, number one,
20 and number two, the watchdog can't later on go and query that data collector
21 for more statistical -- I'm sorry, that bloodhound for more statistical
22 information.

23 He never queries the bloodhound. He waits for the bloodhound to
24 give him a report back. There's no query that's sent out. Basically, the
25 bloodhound agent does its thing, and when it's finished it sends a report back

1 to the watchdog, but there's no query, whereas we have a system where we
2 have, you know, likely hundreds or so of data collectors disbursed
3 throughout a large network. I'd hate to find out how large the network is,
4 and we're constantly, you know, sending queries to various data collectors.
5 We may not send them to all of the data collectors as described in the
6 application, but we're trying to pinpoint the traffic. And the difference
7 between the technique that's described in Yavatkar and what's disclosed
8 here is that we don't rely upon the, the known properties of known types of
9 attacks.

10 Essentially, what we're looking for is irregularities or anomalies in
11 network traffic. We also discuss -- in the specification, we try to compare
12 the statistics to historical information regarding these statistics to try to
13 figure out, you know, where our
14 attacks are coming from and whether or not, in fact, what attack has been
15 launched against the network.

16 Yavatkar can't -- Yavatkar needs to know what the attack is because
17 they have to send out a particular type of bloodhound agent based upon the
18 attack, and we don't have those limitations. So I think that the technique
19 described in Yavatkar and the technique claimed in our claims is quite
20 different, substantially different.

21 So again, I don't -- you know, we have a process described in
22 Yavatkar in which the bloodhound agents follow this -- process which it
23 finds a port for the link that's accepting attack traffic on a node in which the,
24 the bloodhound agent is operating. It tries to traverse that link and to move
25 to the node from the other side of the link and then it repeats the process by

1 the way it moves so the node -- the other side of the link. I guess this is
2 where I'm a little confused in the reference that I believe there is -- it
3 basically launches another bloodhound agent to the other side of that link.

4 But in any event, that's not what we do. We don't have this thing that
5 moves from link to link trying to figure out where, where the traffic is
6 coming from. We basically just have these data collectors deployed in the
7 network and they -- these things are -- you know, basically they are the
8 network and they get queried by a gateway or a control center when there's -
9 - when people suspect there's an attack going on or even proactively to make
10 sure an attack isn't going on.

11 And this is not something that's, that's at all suggested by the
12 Yavatkar reference, much less described by the Yavatkar reference. So in
13 Yavatkar everything that Yavatkar does is predicated on the watchdog agent
14 actually detecting the attack or something else actually detecting an attack.
15 So if there's an attack actually going on in the data center that Yavatkar is
16 trying to detect -- trying to protect, but the watchdog and/or the other thing
17 that detects the attack are not capable of doing it, then that could in -- that
18 could make the attack successful because they need to have -- knowledge or
19 knowledge beforehand of the type of attack that's being launched against the
20 data center.

21 That's not a limitation necessarily in our, our invention. I mean not to
22 say that this invention can detect all possible attacks if some clever attacker
23 would want to launch against the network, but it is clearly not limited to only
24 known types of attacks.

1 The -- so that's the significant advantages of our scheme over that
2 described in the reference, is that by collecting the statistical information on
3 suspicious packet traffic allows us to detect and stop both known and
4 unknown attacks, and whereas the other reference requires that the -- that
5 something already exists that can recognize the attack.

6 So with respect to Claim 1, I -- we believe that the features of sending
7 the queries and the features of, of receiving the statistical information and
8 processing that statistical information to determine the source of suspicious
9 network traffic into the data center is neither described nor suggested by the
10 reference.

11 Claim 2 adds additional feature of, of sending the, the queries to the
12 data collectors for statistical information based on victim destination
13 address. So this obviously is important because in many types of attacks the,
14 the source address of the packet can be spooked. In other words, they're just
15 false addresses. That makes it more difficult to find where the traffic is
16 coming from. However, if you can find data collectors that are receiving --
17 then more easily pinpoint where the attack is coming from.

18 And the Examiner tries to -- that because Yavatkar is concerned with
19 gathering information they somehow describes querying gateways based on
20 victim destination address and the -- I just do not see that in the reference,
21 nor do I see that really in any logical construct of the Examiner's argument.

22 The -- again, what Yavatkar describes is to send reports that detail the
23 path taken during attack, but they don't describe the claim's statistical
24 information and they don't describe getting this information based on
25 attackers that have a destination address for the, for the victim data center.

1 Claim 4 adds the feature of, of a control center that receives statistical
2 information and further adds the features of sending data to and from the
3 gateway that is associated with the victim data center, and there's no
4 mention in the reference of sending data between a gateway and a control
5 center. The data, as required by Claim 4, has it going to and from the
6 control center, so then it is a situation where the gateway device can also be
7 enlisted to develop some of the statistical information and the control center
8 can, can be processing the statistical information that's coming from the
9 gateway device, again sending queries back and forth. That's not described
10 in the reference.

11 Claim 6 adds the feature that the queries and the statistical
12 information are sent over a redundant network. The Examiner never really
13 declared where he considers the redundant network. We give, we give -- in
14 our view, what we describe as a redundant network is a network that is
15 physically separated from the network that is actually carrying the traffic.
16 So one of the problems with the techniques described in Yavatkar is that if
17 in fact the network is under a denial of service attack, a serious attack, the
18 network can be so crowded with traffic that in fact the information that is
19 necessary to determine the source of the attack in the reference could never
20 get to the watchdog to actually do anything with it because it could be stuck
21 in the network based upon the volume of traffic being carried by the network
22 -- have a separate network that can carry that traffic, and that's not, that's
23 not addressed at all in Yavatkar.

24 Claim 9 is directed to the instance in which the source of the attack is
25 behind a gateway and it requires that -- issue a request to the gateway to

1 prevent the attacking traffic from reaching the network. This, this request is
2 issued by the control center. Yavatkar mentions that if the gateway can be
3 identified it can be shut down, but it doesn't describe any actual way to
4 identify the gateway when the source is behind the gateway. He essentially
5 throws that out as a possibility but doesn't describe actually how to do that.
6 We do describe that.

7 Claim 11 -- I, I know I'm getting close to my time. I'm just going to
8 try to finish up as quickly as I can. Claim 11 is -- when the source of the
9 attack is not behind a gateway. And when we query the data collectors that
10 are via logically adjacent the gateway to provide information about a
11 possible locations attacking traffic. And again, Yavatkar does not query the
12 -- their bloodhound agents and does not possess a control center so, so
13 cannot meet any of the functionality described in Claim 11.

14 Finally, 15. Claim 15 up to Claim 1 -- again -- queries the data
15 collectors deployed at different points of the network and the data collectors
16 sample the network pack to collect statistical information and the queries
17 therefore request the statistical information. And again it uses the feature of
18 -- Claim 4 or maybe -- let's see, Claim 2 that the, that the queries are for
19 statistical information from data collectors that examine network traffic with
20 the victim destination address.

21 So in other words, we can use the data collectors to find out where --
22 with the victim destination address are going through and query those data
23 collectors as opposed to data collectors that are not seen that, that network
24 traffic and again try to further pinpoint the source of the attack.

1 And finally I just want to point out to briefly Claim 29 -- scope to --
2 directed to a computer program
3 product residing on a computer readable medium, and it has the feature of
4 receiving a notification of an attack, and that would typically come from, for
5 example, a gateway that though our victim data center believes it's under
6 attack and that would cause the, the scheme to fall into place and again try to
7 use the querying of the data collectors for statistical information and the
8 processing of the statistical information to try to pinpoint the source of the
9 attack.

10 So I have basically, you know, went through the claims I went over
11 today. If you have any questions I'd be happy to entertain them.

12 JUDGE BLANKENSHIP: No, sir, thank you.

13 MR. MALONEY: Okay, thank you very much.

14 JUDGE BLANKENSHIP: We're off the record now --

15 (Whereupon, the hearing concluded at 9:25 a.m. on
16 November 5, 2008.)